AMENDMENTS TO THE CLAIMS:

1. (Original) A system for limiting access to the functionality of one or more software applications, comprising:

a first memory configured to store first data related to each of the one or more software applications;

the first memory further configured to store second data related to each of one or more users of any of the software applications; and

a rules checker in communication with the software applications and the first memory, said rules checker configured to:

receive at least one query, said query originating from any particular one of the software applications, and

forward a message to the particular software application in response to the query;

wherein said message provides instructions to the particular software application regarding entitlements of one of the users to access a particular function of the particular software application.

2. (Original) The system according to claim 1, wherein the first memory is a relational database.

3. (Original) The system according to claim 1, wherein the each of the one or more software applications are implemented on one of a mainframe and a distributed computing system.

4. (Original) The system according to claim 1, further comprising:

a second memory configured to store proprietary data useful to the particular software application, and

wherein said message provides information to the particular software application regarding authorization to output portions of the proprietary data.

5. (Currently Amended) The ~~method~~ system according to claim **1,** wherein the respective first data for each software application includes an identification of hierarchically arranged functions associated with that software application.

6. (Currently Amended) The ~~method~~ system according to claim 5, wherein the query further comprises information relating to the one of the users and relating to at least one of the functions associated with the particular software application, and

wherein the message relates to that one user's authorization to access the at least one function.

7. (Original) The system according to claim 5, wherein the identification of hierarchically arranged functions include functions, sub-functions, and sub-sub functions.

8. (Original) The system according to claim 1, wherein the respective first data for each software application includes an identification of data fields associated with that software application.

9. (Original) The system according to claim 8, wherein the query further comprises information relating to one of the users and relating to at least one of the data fields associated with the particular software application, and

wherein the message relates to that one user's authorization to access the at least one field.

10. (Original) The system according to claim 1, wherein the rules checker is further configured to:

generate the message based on the query, the first data and the second data.

11. (Original) The system according to claim 1, wherein:

the respective second data for each of the users includes at least one role, from among a plurality of roles, associated with that particular user, and

the respective first data for each software application includes:

an identification of hierarchically arranged functions associated with that software application, and

an description of which of the plurality of roles is entitled to access each of the functions.

12. (Original) The system according to claim 11, wherein:

the query includes an identification of a specific one of the users and a specific one of the functions associated with the particular software application;

the rules checker is further configured to generate the message based on the query, the first data and the second data; and

the message instructs the particular software application regarding that specific user's entitlement to access that specific function.

13. (Original) The system according to claim 12, wherein the rules checker logs data relating to an instance in which the specific user is not entitled to access that specific function.

14. (Original) The system according to claim 4, wherein the respective second data for each of the users includes an access level from among a plurality of access levels, associated with that particular user, said access level determining an authorization of that particular user to access proprietary data within the second memory, and

the rules checker is further configured to generate the message based on the query, the first data and the second data.

15. (Original) The system according to claim 1, further comprising:

an administrative application configured to facilitate administration of the first and second data.

16. (Original) The system according to claim 15, wherein the administrative application is further configured to manipulate the first data according to which of a plurality of clients one or more of the users is associated with.

17. (Original) The system according to claim 15, wherein the administrative application is further configured to manipulate the first data according to an identity of a particular one of the users.

18. (Original) The system according to claim 15, wherein the administrative application is further configured to manipulate the first data according to which of a plurality of roles a particular one of the users is associated with.

19. (Original) The system according to claim 15, wherein the administrative application is further configured to manipulate all the first data relating to a specific one of the software applications.

20. (Original) The system according to claim 15, wherein the administrative application is further configured to manipulate all the first data relating to one of a plurality of functions associated with a specific one of the software applications.

21. (Original) The system according to claim 1, further comprising:

an auditing application configured to facilitate auditing of the first and second data and any additional data generated by the rules checker.

22. (Original) The system according to claim 21, wherein the auditing application is further configured to provide a history, upon request, of messages forwarded by the rules checker.

23. (Original) The system according to claim 22, wherein the history emphasizes those messages related to a failed attempt to access the particular function.

24. (Original) The system according to claim 22, wherein the auditing application is further configured to provide a history, upon request, of changes to one or both of the first data and the second data.

25. (Original) A method for providing application-level security, said method comprising the steps of:

storing first data relating to a plurality of software applications;

storing second data relating to a plurality of users of the software applications;

receiving a query from a particular one of the software applications;

in response to the query, forwarding a message to the particular software application, said message providing instructions to the particular software application regarding entitlements of a particular user to access a function of the particular software application.

26. (Original) The method according to claim 25, further comprising the step of:

generating the message based on the query, the first data and the second data.

27. (Original) The method according to claim 26, wherein the query includes an identification of the particular user and the function.

28. (Original) The method according to claim 25, wherein the second data includes for each user, one or more of an associated user ID, client name, role, and business level.

29. (Original) The method according to claim 28, wherein the first data includes for each software application an identification of associated hierarchically arranged functions and characteristics of those users authorized to access each such function.

30. (Original) The method according to claim 29, further comprising the steps of:

correlating the first and second data to determine authorized functions, said authorized functions being those particular functions of each software application which are accessible by a specified user;

generating the message based on the query and the determination of authorized functions, wherein said query includes an identification of the particular user and the function.

31. (Original) The method according to claim 28, wherein the first data includes for each software application an identification of associated data fields and characteristics of entitlements of users to each data field.

32. (Original) The method according to claim 31, further comprising the steps of:

correlating the first and second data to determine authorized data field operations, said authorized operations being those particular operations of each data field which are permitted to a specified user; and

generating the message based on the query and the determination of authorized operations, wherein said query includes an identification of the particular user and of a predetermined data field.

33. (Original) The method according to claim 29, further comprising the steps of:

storing proprietary data useful to one or more of the software applications; and

storing third data relating to accessibility of the proprietary data.

34. (Original) The method according to claim 33, further comprising the steps of:

correlating the first, second and third data to determine authorized data accesses, said authorized data accesses being those particular data accesses of the proprietary data which are permitted to a specified user; and

generating the message based on the query and the determination of authorized data accesses, wherein said query includes an identification of the particular user and of predetermined proprietary data.

35. (Original) The method according to claim 25, further comprising the step of:

creating a log entry relating to the message if the message indicates instructions which prohibit the particular software application access to the function.

36. (Original) The method according to claim 29, further comprising the step of:

administering the first and second data by manipulating one or both of the first and second data according to which of a plurality of clients one or more of the users is associated with.

37. (Original) The method according to claim 29, further comprising the step of:

administering the first and second data by manipulating one or both of the first and second data according to the identity of a particular one of the users.

38. (Original) The method according to claim 29, further comprising the step of:

administering the first and second data by manipulating one or both of the first and second data according to which of a plurality of roles one or more of the users is associated with.

39. (Original) The method according to claim 29, further comprising the step of:

administering the first and second data by manipulating all the first data relating to a specific one of the software applications.

40. (Original) The method according to claim 29, further comprising the step of:

administering the first and second data by manipulating all the first data relating to one of a plurality of functions associated with a specific one of the software applications.

41. (Original) A computer readable medium bearing instructions for providing application-level security, said instructions being arranged to cause one or more processors upon execution thereof to perform the steps of:

storing first data relating to a plurality of software applications;

storing second data relating to a plurality of users of the software applications;

receiving a query from a particular one of the software applications;

in response to the query, forwarding a message to the particular software application, said message providing instructions to the particular software application regarding entitlements of a particular user to access a function of the particular software application.

[[41]] 42. (Currently amended) The system according to claim 14, further comprising:

a non-volatile data store indicating a hierarchical arrangement of the plurality of access levels, and

wherein the rules checker is further configured to consult the data store when determining the authorization of that particular user.

[[42]] 43. (Currently amended) The system according to claim 21, wherein the auditing application is further configured to provide real-time data logging and retrieval.

[[43]] 44. (Currently amended) The system according to claim 2, wherein any updates to data within the relational database are performed in real-time and the rules checker is further configured to use the updated data.

[[44]] 45. (Currently amended) The system according to claim 1, wherein the particular software application is a simulation application, said simulation application is configured to:

provide in the query to the rules checker a simulated user identity and a simulated secured resource identity;

receive from the rules checker the message forwarded by the rules checker; and

determine the entitlements of the simulated user to access the simulated secured resource.

[[45]] 46. (Currently amended) The system according to claim 5, wherein the query requests a listing of entitlements for the one user, said listing identifying the entitlements for every application, function or proprietary data associated with the one user, and wherein the message includes said listing.

[[46]] 47. (Currently amended) The system according to claim [[45]] 46, wherein query includes filtering parameters such that the listing includes only those entitlements which satisfy the filtering parameters.

[[47]] 48. (Currently amended) The system according to claim [[46]] 47, wherein the filtering parameters specify one or more of a user role, a function identity, an application identity, a user identity, and a data access level.

[[48]] 49. (Currently amended) The system according to claim 14, wherein the authorization of the particular user to access proprietary data depends, at least in part, on the particular software application identity.

[[49]] 50. (Currently amended) The system according to claim 14, wherein the authorization of the particular user to access proprietary data depends, at least in part, on the particular function identity.

51. (New) The system of claim 3, wherein the one of the users utilizes a remote system to access the particular function of the particular software application, and is not signed on to the operating system based on which the rules checker operates.

52. (New) The system of claim 1, wherein:

the one of the users is an organization; and

the second data specifies entitlements of the organization to access one or more functions of the particular software application, and entitlements of at least one individual user in the organization to access at least one of the one or more functions of the particular software application that the organization is entitled to access.

53. (New) The system of claim 1, wherein:

the one of the users is an organization having associated proprietary data;

the second data includes an access level associated with an individual user within the organization, wherein the access level is selected from among a plurality of access levels

arranged in a hierarchical structure, and specifies an authorization to access at least part of the proprietary data associated with the organization; and

the individual user is entitled to access all data accessible to an access level hierarchically subordinate to the access level associated with the individual user.

54. (New) The system of claim 53, wherein more than one hierarchical structure is provided, each of the more than one hierarchical structure is associated with a function of the organization, an organization structure of the organization, or geographical regions.

55. (New) The system of claim 53, wherein the access level is assigned to the individual user based on the individual user's role within the organization or the individual user's job function.

56. (New) The system of claim 1, wherein:

the one of the users is an organization having associated proprietary data; and

the second data specifies an authorization granted to an individual user of the organization to access at least part of the proprietary data associated with the organization, based on a function to be performed by the individual user.

57. (New) The system of claim 9, wherein the message includes that one user's authorized action on the at least one field, or the appearance of the at least one field to that one user.

58. (New) The system of claim 1, wherein the entitlements of the one or more users are dynamically configurable without the need to have a specific user to sign-off and sign-on again.

59. (New) The system of claim 1, wherein:

the one of the users is an organization; and

the second data specifies entitlements of the organization to access one or more functions of the particular software application, and entitlements of a role of the organization to access at least one of the one or more functions of the particular software application that the organization is entitled to access; and

a least one individual user of the organization is assignable to the role.